华为认证安全系列教程

HCNP-Security-CSSN

learning. huamei.com/cr 实验指导手册

版本:3.0



小林 华为技术有限公司 版权所有 © 华为技术有限公司 2017。 保留一切权利。

非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部,并不得以任何形式传 播。

商标声明

Wawei和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标,由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束,本文档中描述的全部或部分产品、服务 或特性可能不在您的购买或使用范围之内。除非合同另有约定,华为公司对本文档内容不做任何明示或暗示 的声明或保证。

由于产品版本升级或其他原因,本文档内容会不定期进行更新。除非另有约定,本文档仅作为使用指导,本 文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

文档中的所有陈证	述、信息和建议不构成任何明示或暗示的担保。				
ter ing.					
	华为技术有限公司				
地址:	深圳市龙岗区坂田华为总部办公楼 邮编: 518129				
网址:	http://e.huawei.com				
B. B. S.					



华为认证体系介绍

依托华为公司雄厚的技术实力和专业的培训体系,华为认证考虑到不同客户对网络安全 技术不同层次的需求,致力于为客户提供实战性、专业化的技术认证。

根据网络安全技术的特点和客户不同层次的需求,华为认证为客户提供面向各个方向的 四级认证体系。

HCNP-Security(Huawei Certified Network Professional-Security,华为认证网络高级工程师安全方向)主要面向华为公司办事处、代表处一线工程师,以及其他希望学习华为网络安全产品和网络安全技术的人士。HCNP-Security认证涵盖华为网络安全、内容安全和终端安全的内容。

华为认证协助您打开行业之窗,开启改变之门,屹立在网络安全世界的潮头浪尖!



WE														
必备进阶关		ВС			HCNA	DC		HCNP	DC	>	HCIE	Ы		
-		Big Data			HCNA	Big Data		HCNP	Big Data		HCIE	Big Data		
议进阶关系		Cloud			HCNA	Cloud		HCNP	Cloud		HCIE	Cloud		
- ►		Storage		>	HCNA	Storage		HCNP	Storage		HCIE	Storage	cĊ	
		nication		>	HCNA	VC		HCNP	VC		SW	unication		
		rise Commu	4	>	HCNA	S		HCNP	S	() -` →	HCIE	ise Commu		
	人证全员	Enterpr	HCN	>	HCNA	nc		HCNP	UC			Enterpri		HCA
	华为	LTE		>	HCNA	LIE		HCNP	LTE	>	HCIE	LTE		
		Transmission			HCNA	Transmission		HCNP	Transmission		HCIE	Transmission		
		WLAN		>	HCNA	WLAN		HCNP	WLAN	>	HCIE	WLAN		
13		Security			HCNA	Security		HCNP	Security	>	HCIE	Security		
		R&S					>	HCNP	R&S		HCIE	R&S		
					4	晤工		括他	工系资		家寺休	、铁	!	中的柴



前 言

简介

本书为 HCNP-Security-CSSN 认证培训教程,适用于准备参加 HCNP-Security-CSSN 考试的学员 或者希望了解内容安全过滤,NIP 入侵防御,防病毒攻击,防火墙防单包及流量型攻击等相关 安全技术的读者。

内容描述

本实验指导书共包含 5 个实验,从内容安全过滤开始,逐一介绍了 NIP 入侵防御、服务器防病 毒攻击、用户防病毒攻击、防火墙单包攻击防范、防火墙流量型攻击防范的配置实践。

- 实验一内容安全过滤综合实验,包含文件过滤、邮件过滤、内容过滤、应用行为 控制、URL 过滤,通过配置防火墙安全文件,了解防火墙内容安全的功能及配 置。
- 实验二为 NIP 入侵阻断实验,通过 NIP 直路部署,了解 NIP 的工作原理及配置, 以及如何查看攻击防御记录。
- 实验三为应用服务器防病毒攻击实验,通过部署针对邮件应用服务器的反病毒策略,保护内网服务器不被外网病毒攻击。
- 实验四为用户防病毒攻击实验,通过部署针对客户端的反病毒策略,保护内网用 户不被外网病毒攻击。
- 实验五为防火墙通用防范实验(单包攻击防范),通过在防火墙上部署单包攻击防范,了解防火墙防范单包攻击的原理及配置。
- 实验五为防火墙通用防范实验(流量型攻击防范),通过在防火墙上部署 Anti-DDoS 策略,了解防火墙防范 DDoS 攻击的原理及配置。

读者知识背景

本课程为华为认证中级课程,为了更好地掌握本书内容,阅读本书的读者应首先具备以下基本 条件:

 具有基本的路由交换网络知识背景,同时熟悉华为交换设备,了解基本数通知 识。



本书常用图标









邮件服务器 (SMC)







Web服务器



FTP服务器

网络云2



通用服务器





实验环境说明

组网说明

本实验环境面向准备 HCNP-Security 考试的网络安全工程师。每套实验环境包括防火墙 3 台, 交换机 4 台,路由器 3 台,服务器若干,主机若干。每套实验环境适用于 4 名学员同时上机 操作。

设备介绍

为了满足 HCNP-Security 实验需要,建议每套实验环境采用以下配置:

设备名称、型号与版本的对应关系如下:

1	设备名称	设备型号	软件版本
F	USG防火墙	USG6530	5.160 (USG6500 V500R001C30SPC100)
-	交换机	\$5700	5.130 (S5700 V200R003C00SPC300)
	路由器	AR2200	5.160 (AR2200 V200R007C00SPC900)
	Agile Controller服务 器	Agile Controller	Agile Controller-Campus V100R002C10SPC400
	AnyOffice配套 服务器	AnyOffice	



准备实验环境

检查设备

实验开始之前请每组学员检查自己的实验设备是否齐全,实验清单如下。

设备名称	数量	备注
服务器群组 (HTTP/FTP/Mail/AC/SC/SM/Aanyoffice)	各1台	
华为USG6370防火墙	3台	105
华为S5700交换机	4台	ant
AP4030DN	1个	
虚拟主机	7台	NC'



实验拓扑



拓扑图组建说明:

本实验拓扑模拟了一个小型企业网络。FW1 与 FW2 部署为双机热备组网,作为企业边界设备 控制出口流量。

在企业内网部署了终端用户和服务器资源,并有 NIP 设备监控网络入侵情况。

在企业内部可实现终端安全部署。

在 HCNP-Security v3.0 版本中的实验均在此拓扑中完成。



基础配置说明

实验开始前,需完成各设备的接口地址、安全区域及基本路由信息的相关配置。在后续的实验 中,不再对以上基础信息配置进行说明。

主机登录信息:

名称		管理地址	账户
Server-A	C 172.2	21.20.78/16	Administrator/Admin@123
Server-A	D 172.2	21.20.72/16	Administrator/Auawei@123
Server-FT	P 172.2	21.20.73/16	Administrator/Admin@123
Server-WV	VW 172.2	21.20.74/16	Administrator/Admin@123
Server-M	ail 172.2	21.20.75/16	Administrator/Admin@123
Server-A	E 172.2	21.20.76/16	Administrator/Admin@123
Server-FTP(INT) 172.2	21.20.80/16	Administrator/Admin@123
PC1	172.2	21.20.101/16	admin/Huawei123
PC2	172.2	21.20.102/16	admin/Huawei123
PC3	172.2	21.20.103/16	admin/Huawei123
PC4	172.2	21.20.104/16	admin/Huawei123
PC5	172.2	21.20.105/16	admin/Huawei 123
PC6	172.2	21.20.106/16	admin/Huawei 123
PC7	172.2	21.20.107/16	admin/Huawei 123
PC8 (Attack	PC) 172.2	21.20.108/16	admin/Huawei 123
PC9	172.2	21.20.109/16	admin/Huawei 123
-15-14-135	- 		

设备登录信息:



名称	管理口地址(web/telnet)	账户				
FW1	172.21.20.11/16	admin/Huawei@123				
FW2	172.21.20.12/16	admin/Huawei@123				
FW3	172.21.20.13/16	admin/Huawei@123				
NIP	172.21.20.61/16	admin/Huawei@123				
R1	172.21.20.21/16	Huawei@123				
R2	172.21.20.22/16	Huawei@123				
R3	172.21.20.23/16	Huawei@123				
SW1	172.21.20.31/16	Huawei@123				
SW2	172.21.20.32/16	Huawei@123				
SW3	172.21.20.33/16	Huawei@123				
SW4	172.21.20.34/16	Huawei@123				
AP	172.21.20.51 /16					
防火墙数据规划:						

名称	接口	安全区域	IP Address
	G1/0/1	Trust	10.1.50.11/24
	G1/0/2	DMZ	10.1.61.11/24
FW1	G1/0/3	DMZ	10.1.62.11/24
	G1/0/4	ISP1	10.1.71.11/24
	G1/0/5	ISP2	10.1.73.11/24
	G1/0/1	Trust	10.1.50.12/24
~ K	G1/0/2	DMZ	10.1.61.12/24
FW2	G1/0/3	DMZ	10.1.62.12/24
9	G1/0/4	ISP1	10.1.72.12/24
	G1/0/5	ISP2	10.1.74.12/24
	G1/0/0	Trust	10.1.20.13/24
	G1/0/1	Untrust	10.1.21.13/24
FW3	G1/0/2		10.1.25.13/24
	G1/0/3		10.1.26.13/24
	G1/0/4		10.1.27.13/24

路由器数据规划:



名称	接口	IP Address
	G0/0/1	10.1.71.21/24
R1	G0/0/2	10.1.72.21/24
	E1/0/1	10.1.81.21/24
	G0/0/1	10.1.73.22/24
R2	G0/0/2	10.1.74.22/24
	E1/0/1	10.1.82.22/24

交换机数据规划:

	R2	G0/0/2		10	.1.74.22/24		
		E1/0/1		10	.1.82.22/24		0
交换机数	据规划:						1C1
名私	闭	接口		I	P Address		co ⁿⁿ '
		G0/0/1		10	.1.81.31/24		
		G0/0/2		10	.1.82.31/24	NC	
SW	1	G0/0/3		10	.1.93.31/24		
		G0/0/4		10	.1.92.31/24		
		G0/0/5		10	.1.91.31/24		
		G0/0/1		211	N/A		
SW2	2	G0/0/2	, 10	50-	N/A		
		G0/0/3			N/A		
		G0/0/1		10	.1.10.33/24		
		G0/0/2		10	.1.21.33/24		
		G0/0/3		10	.1.20.33/24		
		G0/0/4		10	.1.40.33/24		
SVV;		G0/0/5		10	.1.50.33/24		
K.K		G0/0/6		10	.1.31.33/24		
5)-		G0/0/7		10	.1.32.33/24		
		G0/0/8		10	.1.33.33/24		
		G0/0/1		10	.1.11.34/24		
		G0/0/2		10	.1.12.34/24		
0.44		G0/0/3					
SVV4	4	G0/0/5					
		G0/0/6		10	.1.13.34/24		
		G0/0/7		10	.1.10.34/24		



设备预配脚本

本实验手册基于综合拓扑完成。各设备均包含预配信息,如果重置了环境,请按如下预配信息 设置基本信息。设备密码均为 Huawei@123。

实验验证文件

序号	实验	验证文件
1	文件过滤实验	test.exe
2	邮件过滤实验	test.mp4
3	应用行为控制实验	test.mp4
4	应用服务器防病毒攻击实验	eicar_com.zip
5	内网用户防病毒攻击实验	eicar_com.zip



目录

前 言	iv
简介	iv
内容描述	iv
读者知识背景	iv
本书常用图标	V
实验环境说明	v
准备实验环境	vi
1 实验一:内容安全过滤综合实验	xv
1.1 实验介绍	xv
1.1.1 关于本实验	xv
1.1.2 实验目的	xv
1.1.3 实验拓扑图	
1.1.4 前提条件	
1.1.5 实验规划	xvi
1.1.6 实验任务列表	xviii
1.2 实验任务配置	xviii
1.2.1 配置思路	
1.2.2 任务一: 文件讨滤	
123 任务 ^一 : 内容过速	xxiii
124 任冬三:邮件过速	XXV
125 任冬四:应田行为控制	xxvii
1.2.5 任为百. 应用目为正的	vviv
12.0 任务工. 016 及滤	
1.5 癿直学与 2 NID λ 得阳概 守逊	
21 页译的天空	
2.1 头短川珀	
2.1.1 大丁平头拉	
2.1.2 头粒日的	
2.1.3 头验狗扑图	
2.1.4 前提杀件	



	2.1.5 实验任务列表	
	2.2 实验任务配置	
	2.2.1 配置思路	
	2.2.2 配置步骤	
3	应用服务器防病毒攻击实验	
	3.1 实验介绍	
	3.1.1 关于本实验	
	3.1.2 实验目的	
	3.1.3 实验拓扑图	
	3.1.4 前提条件	
	3.1.5 实验规划	43
	3.1.6 实验任务列表	
	3.2 实验任务配置	
	3.2.1 配置思路	
	3.2.2 配置步骤	
	3.3 结果验证	
	3.4 配置参考	
	3.4.1 FW 的配置	
4	内容用户防病毒攻击实验	51
	4.1 实验介绍	51
	4.1.1 关于本实验	51
	4.1.2 实验目的	51
	4.1.3 实验拓扑图	51
	4.1.5 前提条件	52
	4.1.6 实验规划	52
	4.1.7 实验任务列表	52
	4.2 实验任务配置	53
	4.2.1 配置思路	53
	4.2.2 配置步骤	53
	4.3 结果验证	56
	4.4 配置参考	56



	4.4.1 FW 1 的配置	
5	防火墙单包攻击防范实验	
	5.1 实验介绍	
	5.1.1 关于本实验	
	5.1.2 实验目的	
	5.1.3 实验拓扑图	
	5.1.4 前提条件	
	5.1.5 实验任务列表	
	5.2 实验任务配置	
	5.2.1 配置步骤(任务一)	
	5.3 结果验证	
	5.3.1 查看防火墙的日志	
	5.4 配置参考	61
	5.4.1 FW1 的配置	61
6	防火墙流量型攻击防范实验	
	6.1 实验介绍	
	6.1.1 关于本实验	
	6.1.2 实验目的	
	6.1.3 实验拓扑图	62
	6.1.4 前提条件	
	6.1.5 实验任务列表	63
	6.2 实验任务配置	
	6.2.1 配置步骤	63
	6.3 结果验证	64
	6.3.1 查看防火墙的日志	64
	6.4 配置参考	65
	6.4.1 FW1 的配置	65



实验一:内容安全过滤综合实验

1.1 实验介绍

1.1.1 关于本实验

某公司在网络边界处部署了 FW 作为安全网关。公司希望在保证网络能够正常使用的同时实现以下需求:

- 为了防止公司机密文件的泄露,禁止员工上传常见文档文件、代码文件(C、 CPP、JAVA)以及压缩文件到 Internet 服务器;
- 为了降低病毒进入公司内部的风险,禁止员工从 Internet 下载可执行文件以及 Internet 用户上传可执行文件到内网服务器;
- 公司希望在保证网络正常使用的同时,防止内部员工泄露公司机密信息;
- 公司规定发送往外网或接收来自外网的邮件单个附件均不能超过 2M;
- 公司希望员工上传和下载的文件大小不能超过 2M;
- 外网网站 http://10.1.92.80 疑似有安全隐患,内网员工不能访问该网站且不能访问 社交网络等网站。

1.1.2 实验目的

- 掌握文件、内容、邮件过滤以及应用行为控制的应用场景;
- 掌握文件、内容、邮件过滤的配置方法。
- 1.1.3 实验拓扑图



图1-1 内容安全过滤综合实验拓扑图



- 1.1.4 前提条件
 - 1. 配置防火墙网络连接、IP 地址、接口安全区域。
 - 2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
 - 3. NAT 策略部署完成。
- 1.1.5 实验规划

表1-1 实验数据规划

项目	数据	说明
安全策略 to_Internet	名称: to_Internet 源安全区域: trust 目的安全区域: isp1 动作: 允许 文件过滤: profile_file_1 内容过滤: profile_data_1 邮件过滤: profile_mail_1 应用行为: profile_app_1	安全策略"to_Internet" 的作用是允许公司员 工访问 Internet。



安全策略 to_intra_server	名称: to_intra_server 源安全区域: isp1 目的安全区域: trust 目的地址: 10.1.32.0/24 动作: 允许 文件过滤: profile_file_2 邮件过滤: profile_mail_1	安全策略 " to_intra_server"的作 用是允许外网用户访 问内网服务器。
文件过滤	名称:rule1 文件类型:文档文件、代码文件、压缩文件 方向:上传 动作:阻断	禁止员工上传文档、 开发和压缩文件到 Internet。
profile_file_1	名称: rule2 文件类型:可执行文件 方向:下载 动作:阻断	禁止员工从 Internet 下 载可执行文件。
文件过滤 profile_file_2	名称: rule1 文件类型:可执行文件 方向:上传 动作:阻断	禁止 Internet 向内网服 务器上传可执行文件
内容过滤 profile_data_1	名称: rule1 关键字: key1 应用: all 文件类型: all 方向: 上传 动作: 阻断	阻断关键字为 key1 的 内容的上传。
邮件过滤 profile_mail_1	控制项: 垃圾邮件过滤 发送/接收附件大小限制:2M	防止垃圾邮件并控制 附件单个附件大小不 超过 2M。
应用行为控制 profile_app_1	控制项: FTP 上传/下载阻断阈值 100M	文件超出 100M 会执 行阻断



URL 过滤	自定义 URL 分类,将 HTTP://10.1.92.80 网	禁止访问
Profile_URL_1	站设置为禁止访问。	http://10.1.92.80

1.1.6 实验任务列表

序号	任务	子任务	任务说明
		文件过滤	禁止员工上传常见文档文件、代码文件(C、 CPP、JAVA)以及压缩文件到Internet服务器; 禁止员工从Internet下载可执行文件以及 Internet用户上传可执行文件到内网服务器
1	内容安全过滤 配置文件	内容过滤	防止内部员工泄露公司机密信息
		邮件过滤	邮件发送接收单个附件均不能超过2M
		应用行为控制	上传和下载的文件大小不能超过100M
		URL过滤	禁止访问外网网站http://10.1.92.80
2	安全策略	内网用户访问 Internet	配置安全策略并调用文件过滤、内容过滤、 邮件过滤、应用行为控制以及URL过滤以满足 需求
		外网用户访问 内网服务器	配置安全策略并调用文件过滤和邮件过滤以 满足需求

1.2 实验任务配置

1.2.1 配置思路

- 1. 基本网络参数配置;
- 2. 网络地址转换配置。
- 3. 内容安全过滤文件配置;
- 4. 安全策略配置引用内容安全配置文件;

1.2.2 任务一: 文件过滤

步骤1 文件过滤配置文件。

1) 选择"对象>安全配置文件>文件过滤>文件过滤配置文件"。在文件过滤规则菜单中,单 击"新建",新建文件过滤配置文件 profile_file_1,点击"新建",新建文件过滤规则。



新建文件过渡	配置文件							?	×
名称 描述	profile_file_	1			*				
文件过滤规	则								
🕂 新建 🗱	刪除 💲移动								
□ 名称	应用	文件类型	自定义扩展名	方向	动作	DSCP优先级	编辑		

a. 新建规则1阻断文档文件、代码文件、压缩文件的上传。

新建文件过滤规则	? ×	
名称	rule1 *	
应用	全部 🔽 *	
文件类型	DOC, PPT, XLS, MSOFFICE, DOCX, PPTX	
自定义扩展名	hushe	
方向	上传	
动作	阻断 说明: IMAP与NFS不支持阻断动作,将对其执行告 警动作。	
	确定取消	

b. 新建规则 2 阻断可执行文件下载



新建文件过滤规则		? ×
名称	rule2	*
应用	全部	*
文件类型	EXE,MSI,RPM,OCX,A,ELF,DLL,PE,SYS	. 🗸
目定义扩展名		
方向	下载	~
动作	阻断	~
	说明: IMAP与NFS不支持阻断动作,将对 警动作。	対其执行告
	确定	取消

c. 点击"确定"。

修改文件过	悲配置文件			0		?
名称 描述	profile_file	_1	- 60	•		
文件过滤规	LQI					
🕂 新建 📁	删除 💲移动					
2 名称	应用	文件类型 自定义	扩展名 方向	动作	DSCP优先级	编辑
🗌 rule1	全部	DOC, PPT, XLS, MSO	上传	阻断		
🗌 rule2	全部	EXE,MSI,RPM,OCX,	下载	阻断		
	XX					共2条
-1.					đ	角定 取洋
2) 新建 a. 点音	建文件过滤 击"新建"。	愿配置文件"profile_	file_2"。			
· · · · · · · · · · · · · · · · · · ·						

新建文件过滤配置	文件							?	×
名称	profile_file_2				*				
描述]				
文件过滤规则									
🕂 新建 💥 删除	💲 移动								
名称 应	用	文件类型	自定义扩展名	方向	动作	DSCP优先级	编辑		

新建规则1阻断可执行文件上传 b.



新建文件过滤规则	? ×	
名称	rule1 *	
应用	全部 🗸 *	
文件类型	EXE,MSI,RPM,OCX,A,ELF,DLL,PE,SYS 🔽	
自定义扩展名		
方向	上传	
动作	阻断	
	说明: IMAP与NFS不支持阻断动作,将对其执行告。 警动作。	
	确定取消	

步骤2 安全策略引用内容安全配置文件。

1) 选择"策略>安全策略",单击新建安全策略"to_Internet",用于允许内网用户访问外网, 并引用文件过滤配置文件 profile_file_1。



所建安全策略					? ×
是示: 新建时可以基于策略模板来快速定>	X您需要的策略。[选择策略	模板			-
3称	to_internet		*		
苗述					
範組	NONE	~			
原安全区域	trust	N	/ [多选]		
目的安全区域	isp1	~	/ [多选]		
原地址/地区?	10.1.11.0/24				
目的地址/地区②	请选择或输入地址				
1户??	请选择或输入用户		[多选]		
接入方式 🕐	请选择接入方式				
终端设备 🕐	请选择终端设备				
服务	请选择服务				
立用	请选择应用或应用组		[多选]		
寸间 段	any	N	~		
力作	• 允许	○ 禁止			
内容安全	[
	NONE	~	/ [][][][]][]][]][]][]][]][]][]][]][]][]]		•
人侵防御	NONE	~	• [][][]][][]][]][]][]][]][]][]][]][]][]]		
URL过滤	NONE	~	/ [][][][][][][][][][][][][][][][][][][]	1.	
文件过滤	profile_file_1	~	- [四]置]		
内谷过源	NONE	~	/ [][][][][][][][][][][][][][][][][][][]	1	
应用行为控制	NONE	~	• [][[]][[]][[]][[]][[]][[]][[]][[]][[]]		
邮件过滤	NONE	~			
APT防御	NONE	~			
己录策略命中日志	启用				
已录会话日志	启用				
话老化时间		<1-65535>秒			
1定义长连接(?)	启用				
	168	*<0-24000>/]अत्र			
		· ·			•
			[确定取	!消

2) 新建安全策略"to_intra_server",用于允许外网用户访问内部服务器,并引用文件过滤配置文件 profile_file_2。



新建安全策略				? ×
提示:新建时可以基于策略模板来快速	定义您需要的策略。选择	释策略模板]	1	-
	to_intra_server		*	
油 还				
東船狙	NONE	~		
	isp1	~	[多选]	
目的安全区域	trust	~	[多选]	
源地址/地区(?)	请选择或输入地址			
目的地址地区(?)	请选择或输入地址			
用户(?)	请选择或输入用户		[多选]	
接入方式(?)	请选择接入方式			
终端设备 🕐	请选择终端设备			
服务	请选择服务			
应用	请选择应用或应用纠	1	[多选]	10
时间段	请选择时间段	\checkmark		
动作	• 允许	○ 禁止		
内容安全				
反病毒	NONE	~	酉(置)	
入侵防御	NONE	\checkmark	[四]置]	
URL过滤	NONE	~	酉(置)	
文件过滤	profile_file_2	\checkmark	画(王)	
内容过滤	NONE	\sim	酉(置)	
应用行为控制	NONE		西(置)	
邮件过滤	NONE		酉(置)	
APT防御	NONE		酉(置)	
记录策略命中日志	启用			
记录会话日志	启用			
会话老化时间		<1-65535>秒		
自定义长连接?				
	168	*<0-24000>小时		
				•
				确定 取消

步骤3 提交配置。

步骤4 结果验证。

- 内网用户 PC1 无法上传常见文档文件、代码文件(C、CPP、JAVA)以及压缩文件 到 Internet 上的 FTP server;
- 内网用户 PC1 无法从 Internet 上的 FTP server 下载可执行文件;
- Internet 用户 PC9 不能上传可执行文件到内网 FTP 服务器;

1.2.3 任务二: 内容过滤

步骤1 内容过滤配置文件。

1) 选择"对象>关键字组>新建",新建关键字组 key1。新建自定义关键字"公司违规信息"。





2) 新建内容过滤配置文件"profile_data_1"。新建内容过滤规则阻断内容匹配关键字 key1 的 文件上传。

新建内容过新	意配置文件							?
名称 描述	profile_data_1			*				
内容过滤规								
♣新建 🞇	刪除							
名称	关键字组	应用	文件类型	方向	动作	告警讕值	阻断阈值	编辑
🗌 rule	kev1	全部	全部	上传	阳康府			

步骤2 安全策略引用内容安全配置文件。

1) 选择"策略>安全策略",单击新建安全策略"to_Internet",用于允许内网用户访问外网, 并引用内容过滤配置文件 profile_data_1。



新建安全策略		? ×
提示: 新建时可以基于策略模构	反来快速定义您需要的策略。[选择策略模板]	^
谷称	to_internet	*
1田)企		
東船組	NONE	
	trust	9通
目的安全区域	isp1	❷选
源地址/地区(?)	请选择或输入地址	
目的地址地区(?)	请选择或输入地址	
用户(?)	请选择或输入用户	
接入方式	请选择接入方式	
终端设备③	请选择终端设备	
服务	请选择服务	
应用	请选择应用或应用组	[多选]
时间段	any	
动作	 允许 	○禁止
内容安全 反病毒	NONE	
入侵防御	NONE	
URL过滤	NONE	
文件过滤	NONE	
内容过滤	profile_data_1	
应用行为控制	NONE	
邮件过滤	NONE	[] [] [] [] [] [] [] [] [] [] [] [] [] [
APT防御	NONE	▶ [] [] [] [] [] [] [] [] [] [] [] [] []
记录策略命中日志		
记录会话日志		
会话老化时间	<1-65535>秒	
自定义长连接?		
	168 ★<0-24000>/]\9	и ад
		×
		确定 取消

步骤3 提交配置。

步骤4 验证结果。

• 内部员工 PC1 无法上传包含关键字的公司文件到 Internet 上的 FTP server;

1.2.4 任务三:邮件过滤

步骤1 邮件过滤配置文件。

选择"对象 > 安全配置文件 > 邮件过滤"。新建邮件内容过滤文件,过滤垃圾邮件并阻止单个邮件附件大小超过 2M 的文件发送和接收。



新建邮件内容过滤配置文件			?	×	
名称 profile_mail_1		*			
描述					
✔ 垃圾邮件过滤					
发送匿名邮件	允许 🗸				
接收匿名邮件	允许 🗸				
邮件地址组 MIME标题组					
控制方向 控制选项 邮件地址	组		处理动作 编辑		
发送邮件 发件人地址					
收件人地址					
接收邮件 发件人地址					
收件人地址			2		
			共 4 条		
				-	
▲ 附件大小及个数控制					
✔ 发送附件个数上限 3 10	<0-10>	处理动作 告警	\sim		
✓ 按收附件本数上限 ② 10	<0.105	小理动作 生物		2	
	×0*10×				
✔发送附件大小限制 2048	<1-20480>(单位: KB)	处理动作阻断			
		hum-h/t andr			
✓ 接收附件大小限制 ③ 2048	<1-20480>(単位: KB)	XCIEANIE REEL			
	1111 /- 1149-1 /L	· ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~			
说明: IMAP协议不支持阻断动作,将S	具执行告警动作。			•	
			确定 取消		

步骤2 安全策略引用内容安全配置文件。

1) 新建安全策略"to_intra_server",用于允许外网用户访问内部服务器,并引用邮件过滤配置文件 profile_mail_1。



#于: 新總时可以還于錦崗樓報朱快速定义恋葉要的論題。 15/3 編輯	新建安全策略			? ×	
全部 bu_intra_server 新闻 NONE 第次全区场 1591 自治安全区域 1591 自治安全区域 1591 自治安全区域 1591 自治安全区域 1591 自治安全区域 1591 自治安全区域 1591 第地地地区② 1564年30人地址 日的地址地区③ 1564年30人方式 第人方式③ 1564年30人方式 浅湖大各省③ 1564年30人方式 第次方式③ 1564年30人方式 第次方式③ 1564年30人方式 第次時 1564年30人方式 日日段 1564年30人方式 第 1564年30人方式 第 1564年30月20日 5/31 1564年30月20日 157 1564年30日 158 - NONE 158 - 0-2400-7441 <th>提示: 新建时可以基于策略模板</th> <th>来快速定义您需要的策略。[选择策略模板]</th> <th></th> <th>1</th> <th></th>	提示: 新建时可以基于策略模板	来快速定义您需要的策略。[选择策略模板]		1	
超过 - NONE - ● 原安全区域 191 ● 5/31 目的安全区域 1031 ● 5/31 夏地址均区③ 南法探索输入地址 ● 5/31 日的安全区域 1032 ● 5/31 夏地址均区③ 南法探索输入地址 ● 5/31 日的按址均区④ 南法探索输入地址 ● 5/31 日前 ● 5/31 ● 5/31 月戶④ 唐法探索输入用户 ● 5/31 市 ● 5/31 ● 5/31 市 ● 5/31 ● 5/31 町段 ● 5/14 ● 5/31 町房 ● 5/31 ● 5/31 </th <th>名称</th> <th>to_intra_server</th> <th>*</th> <th></th> <th></th>	名称	to_intra_server	*		
第昭祖 - NONE - ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	描述				
調査症 [pp1] 「「」」」」」」 [5/3] 開始安全区域 「11041 「11041 「11041 「11041 「11041 「11041 [110411 [110411 <td>策略组</td> <td> NONE</td> <td>\checkmark</td> <td></td> <td></td>	策略组	NONE	\checkmark		
目的安全区城 「wusi ● 珍述 那些山地虹区③ 雨这程梁编入地址 日的地北地区③ 雨这程梁编入地址 日的北北地区③ 雨这程梁编入地址 日户● 商这程梁编入地址 日本 商这程梁编入地址 日本 商这程梁编入地址 日本 商这程梁编入地址 日本 商送程编方式 「該小方式③ 商送程编方式 「「該合理编》 ● 「「該是福道集」 ● 「「「「「「」」」」 ● 「「「」」」」 ● 「「」」」」 ● 「「」」」 ● 「「」」」」 ● 「「」」」」 ● 「」」」」 ● 「」」」 ● 「」」」」 ● 「」」」 ● 「」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 「」」 ● 「」」 ● 「」」」 ● 「」」」 ● 「」」」 ● 」」」 ●	源安全区域	isp1	▶ [多选]		
第他地地区 ③ 请选择或输入地址 目的地址地区 ④ 请选择或输入地址 日户 ④ 请选择或输入用户 第人方式 ④ 请选择或输入用户 第人方式 ④ 请选择或输入用户 「新人」「「「」」」」」」 「「」」」」 「「」」」」 「」」」」 「「」」」」 「」」」 「「」」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」」 「」」」 「」」」」 「」」」 「」」」」 「」」」 「」」」 「」」」 「」」」」 「」」」 「」」」」 「」」」 「」」」」 「」」」 「」」」 「」」」 「」」」」 「」」」	目的安全区域	trust	▶ 修选]		
副約地址地吃② 請法経知输入規止 用户③ 请法経政输入規止 用户④ 请法経政治入用户 「請法経政治入方式 「該法経政治入方式 受法 请法経知入方式 受法 请法経知入方式 受法 请法経知入方式 受法 请法経知為定品 勝方 「请法経政治規定品 成方 「請法経知問規定品 「「請注理知問股 ● 动作 ・ かけ 「「「「「「」」」」 ● 八〇四万前 ● 八〇四万前 ● 「「「」」」 ● 八〇四万前 ● 「「」」 ● 「「」」 ● 「「」」 ● 「「」」 ● 「「」」 ● 「「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ● 「」」 ●	源地址/地区??	请选择或输入地址			
開户● 请送福班輸入用户 ● 送 散入方式● 请送福祉入方式 就場後音● 请送福祉券 勝ろ 请送福服券 四月 请送福助月館 ● 送 时間記 请送福助月館 ● 送 討館 「方法 ● 受 討印 「読法報告報告報 ● ジ 問題記 「読法報助月館 ● ジ 訪市 ● 方は ● 禁 「「市客女 ● 方は ● 禁 「小市 ● 「回 ● ご 以は返 ● 小いNE - ● 回 いいNE - ● 回 ● 回 いいNE - ● 回 ● 回 いいNE - ● 回 ● 回 「市行が注想 ● NONE - ● 回 「市行が活動 ● NONE - ● 回 「記 ● 「日 ● (1-5535-刊) 「記 ● (1-24000-)「ぼ ● ● 「記 ● (-24000-)「ぼ ● ● 「 ● (-24000-)「ぼ ● ●	目的地址/地区(?)	请选择或输入地址			
強人方式	用户⑦	请选择或输入用户	[多选]		
Kumpe ● 前法程級損役备 前法 # M m m m m m m m m m m m m m m m m m m	接入方式(?)	请选择接入方式			
勝秀	终端设备 🕐	请选择终端设备			
函用 ● 送着应用或应用组 ● 送着 时间段 ● 适法指时间段 ● 动作 ● 允许 ● 禁止 小 ● 小 ● 禁止 小 ● 公 ● 読品 ○ ● 介许 ● 禁止 ○ ● 介白 ● ○ ○ ● 介白 ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ ○ ● ○ ● ○ <td>服务</td> <td>请选择服务</td> <td></td> <td></td> <td></td>	服务	请选择服务			
时间段 前选择时间段 ● 訪休 ● 允许 算止 「内容安全 ⑤病亭	应用	请选择应用或应用组	[多选]		
ホ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	时间段	请选择时间段	~		
内容安全	动作	• 允许	○ 禁止		
反病毒 NONE ● 図習 入侵防御 NONE ● 図習 URL过速 NONE ● 図習 文件过速 NONE ● 図習 内容过速 NONE ● 図習 应用行为控制 NONE ● 図習 邮件过速 profile_mail_1 ● 図習 邮件过速 profile_mail_1 ● 図習 心泉余略命中日志 自用 记录余语日志 自用 台話老(松前间 <1-65535>秒 自定义长连接@ 自用 168 ★-0-24000>/JBł ●	内容安全				
入侵防御 NONE ● 配置 URL过速 NONE ● 配置 文件过速 NONE ● 配置 内容过速 NONE ● 配置 应用行为控制 NONE ● 配置 邮件过速 profile_mail_1 ● 配置 邮件过速 profile_mail_1 ● 配置 心え発菜略命中日志 自用 ごえ完菜略命中日志 自用 ごえ会話日志 自用 台話老化切詞 <1-86535>秒 自定义长连接 ● 自用 168 ★-0-24000>/JBł	反病毒	NONE	▶ 酉(置)		
URL过滤 NONE ● 回置 文件过滤 NONE ● 回置 内容过滤 NONE ● 回置 应用行为控制 NONE ● 回置 邮件过滤 profile_mail_1 ● 回置 APT防御 NONE ● 回置 记录余略命中日志 自用 记录会话日志 自用 会话老(化时间 <1-85535>秒 自定义长连接④ 自用 168 +-0-24000>/1%	入侵防御	NONE	▶ 酉(置)		
文件过速 NONE ● 回置 内容过速 NONE ● 回置 应用行为控制 NONE ● 回置 邮件过速 profile_mail_1 ● 回置 邮件过速 profile_mail_1 ● 回置 必用下防御 NONE ● 回置 记录策略命中日志 自用 会话名北印间 <1-65535>秒 自定义长连接 ● 自用 168 <0-24000>/181	URL过滤	NONE	▶ 酉(置)		
内容过速 NONE ● 図話 应用行为控制 NONE ● 図話 邮件过速 profile_mail_1 ● 図話 APT防御 NONE ● 図話 记录前略命中日志 自用 记录会话日志 自用 会话老化时间 <-1.65535>秒 自定义长连接③ 自用 188 -<0-24000>/Jsh	文件过滤	NONE	▶ [四]]		
应用行为控制 NONE ■ 回流 邮件过速 profile_mail_1 ■ 回流 APT防御 NONE ■ 回流 记录策略命中日志 自用 记录会话日志 自用 会话老化时间 自定义长连接③ 自用 188 +0-24000-/J-Bł	内容过滤	NONE	▶ 酉(置)		
邮件过滤 profile_mail_1 ■ ■ APT防御 ~·NONE ■ 记录範略命中日志 自用 □ 记录会话日志 自用 会话老化时间 自定义长连接 ? □ □ 188 *<0-24000>-/J-Bit ▼	应用行为控制	NONE	▶ 酉(置)	\mathcal{A}	
APT防御 ·· NONE 歐置 记录策略命中日志 自用 记录会话日志 自用 会话老化时间 <1-65535>秒 自定义长连接 ? 自用 188 *<0-24000>/j.kj 確定<	邮件过滤	profile_mail_1			
记录策略命中日志 自用 记录会话日志 自用 会话名(他时间 <1-65535>秒 自定义长连接④ 自用 168 ★-0-24000>/\\$t]	APT防御	NONE	[置酒]		
记录会话日志 自用 会话老化时间 自定义长连接? 自用 168 ★<0-24000>小时	 记录策略命中日志	□ 启用			
会话老化时间 <1-65535>秒 自定义长连接③ 168 ★<0-24000>小时 <	记录会话日志	启用			
自定义长连接 ⑦ □ 启用 168 ★-0-24000>小时	会话老化时间	<1-65535	5≻秒		
168 *<0-24000>/小时	自定义长连接 🕐				
			0>小时		
确定即消				•	
10011				确定取消	

- 步骤3 提交配置。
- 步骤4 结果验证。
 - PC9不能发送单个附件超过 2M 的邮件到内网;
 - PC1 发送超过 2M 附件的邮件, PC9 无法接收。
- 1.2.5 任务四:应用行为控制

步骤1 应用行为控制配置文件。

1) 选择"对象 > 安全配置文件 > 应用行为控制"。新建应用行为控制配置文件, 阻断 FTP 上传和下载大小超过 2M 的文件。



新建应用行	方控制配置文件			?	×
名称	profile_app_1			•	
猫还					
▼ HTTP行	为控制				
▲ FTP行ク	的控制				
FTP 文件上	传	● 允许	○ 禁止		
告警诫(直		<1-4096000>KB		
阻断阈值	Ē	2048	<1-4096000>KB		
		备注:告警阈(- 直必须小于阻断阈值。		c
FTP 文件T	「载	• 允许	○ 禁止	61	
告警谳(ā.		<1-4096000>KB		
阻断阈值	Ξ.	2048	<1-4096000>KB		
		备注:告警阈(- 直必须小于阻断阈值。		
FTP 文件册	削除	● 允许	○ 禁止		

步骤2 安全策略引用内容安全配置文件。

1) 选择"策略>安全策略",单击新建安全策略"to_Internet",用于允许内网用户访问外网, 并引用内容安全配置文件。



新建安全策略				? ×
提示:新建时可以基于策略模板来快	速定义您需要的策略	。[选择策略模板]		_
名称	to_internet		*	
描述				
策略组	NONE	\checkmark		
源安全区域	trust	\checkmark	[多选]	
目的安全区域	isp1	\checkmark	[多选]	
源地址/地区 🕐	请选择或输入	地址		
目的地址/地区 🕐	请选择或输入	地址		
用户(?)	请选择或输入	用户	[多选]	
接入方式 🕐	请选择接入方	式		
终端设备 🕐	请选择终端设	备		
服务	请选择服务			
应用	请选择应用或	应用组	[多选]	
时间段	any	\checkmark		
动作	● 允许	○ 禁止		
内容安全				
反病毒	NONE	\checkmark	酉(置)	
入侵防御	NONE	\checkmark	酉(置)	
URL过滤	NONE	\checkmark	四(置)	
文件过滤	NONE	\checkmark	[置]置]	
内容过滤	NONE	\checkmark	[置]置]	
应用行为控制	profile_app_	1	[置][置]	
邮件过滤	NONE		[][[]][[]][[]][[]][[]][[]][[]][[]][[]]	
APT防御	NONE		酉(置)	
记录策略命中日志	自用			
记录会话日志	自用			
会话老化时间		<1-65535>秒		
自定义长连接?		<u>, 0</u>		
	168	*<0-24000>小时		
				确定取消

步骤3 提交配置。

步骤4 验证结果。

- 内网用户 PC1 无法上传大小超过 2M 的文件到外网的 FTP 服务器;
- 内网用户 PC1 无法从外网 FTP 服务器上下载大小超过 2M 的文件;

1.2.6 任务五: URL 过滤

步骤1 URL 过滤配置文件。

1) 选择"对象 > URL 分类",新建一条自定义 URL 分类。单击确定完成配置。



新建URL分	×		?	×
名称	user_defined_url			*
描述				
URL(?)	10.1.92.80			
HOSTO				
11001				
				59
		确定	取消	

2) 选择"对象 > 安全配置文件 > URL 过滤"。新建一条 URL 过滤配置文件。在 URL 过滤级 别一栏选择自定义,将前一步骤中创建的 URL 分类设置为阻断,并按如图所示将社交网 站等设置为阻断。



修改URL过滤配置文件						?
名称	Profile LIRI	1	*			
描述						
动作模式⑦	• 严格	○ 松散				
缺省动作	允许		\checkmark			
恶意URL检测	自用					
类型	白名单			黒名单		
白名单的优先级	高于黑名单		白名单的优先	级高于黑名单		
URL (?)						
Ŭ						
白名单的优先级	高于黑名单		白名单的优先	级高于黑名单		
HOST						olli,
						G
URL过滤级别						
 高 对所有 	成人网站,非法活动),社交网络,视频	共享等网站进行严格	的限制。	18	3
○ 中 对所有 ○ 任 対命機	成人网站和非法网站 网站进行场制。	进行控制。				
	1934A21111101~					
名称	〇 允许	○ 告警		重标记报文优先级		
▷ 自定义分类 ?	0	0	۲	NONE	\sim	
⊳ P2P		۲	0	NONE	\checkmark	
▷ 下载	0	۲	0	NONE	\checkmark	
▷ 人文	۲	0	0	NONE	\checkmark	
▷ 体育/运动	۲			NONE	\checkmark	
▷ 社会焦点	۲	0	0	NONE	\checkmark	
▷ 军事	۲			NONE	\checkmark	
▷ 社交网络	0	0	۲	NONE	\checkmark	
▷ 博彩		XX	۲	NONE	\checkmark	
▷ 休闲			۲	NONE	\checkmark	
▷ 宗教/超自然	0		۲	NONE	\sim	
▷ 性题材	0	0	۲	NONE	\sim	
▶ 房产家居	0	0	۲	NONE	\sim	
IN THE RESIDE		0	0	NONE		

步骤2 安全策略引用内容安全配置文件。

1) 选择"策略>安全策略",单击新建安全策略"to_Internet",用于允许内网用户访问外网, 并引用内容安全配置文件。



提示:新建时可以基于策略模构	反来快速定义您需要的策略。[选择策略模板]		-	
名称	to_internet	*		
描述				
策略组	NONE	\checkmark		
源安全区域	trust	▶ [多选]		
目的安全区域	isp1	▶ [多选]		
源地址/地区🕐	请选择或输入地址			
目的地址/地区🕐	请选择或输入地址			
用户(?)	请选择或输入用户	[多选]		
接入方式 🕐	请选择接入方式			
终端设备 🕐	请选择终端设备			
服务	请选择服务			
应用	请选择应用或应用组	[多选]		
时间段	any	~		
动作	• 允许	○ 禁止		
内容安全				
入月时初	NONE		+	
	NONE			
ORL(1)版 在/H1+/在	profile_url_1			
又件过滤	NONE			
内合过滤	NONE			
应用行为控制 	NONE			
田川千辺忠	NONE		*	
APT防御	NONE	[] [] [] [] [] [] [] [] [] [] [] [] [] [
记录策略命中日志	启用			
记录会话日志	启用			
会话老化时间	<1-6553	5>秒		
自定义长连接?	□启用			
	168 *<0-240	00>小时		
			•	
			确定 取消	

- 步骤3 提交配置。
- 步骤4 验证结果。
 - 在 PC1 上无法访问 http://10.1.92.80

1.3 配置参考

```
sysname FW1
#
interface GigabitEthernet1/0/1
    undo shutdown
    ip address 10.1.50.11 255.255.255.0
#
interface GigabitEthernet1/0/4
    undo shutdown
    ip address 10.1.71.11 255.255.255.0
#
firewall zone trust
    set priority 85
```



```
add interface GigabitEthernet1/0/1
 #
firewall zone name isp1
  set priority 40
  add interface GigabitEthernet1/0/4
#
 firewall interzone trust isp1
  detect ftp
 #
profile type app-control name profile_app_1
  http-control file direction upload block-size 102400
  ftp-control file direction upload block-size 102400
  ftp-control file direction download block-size 102400
 #
 profile type file-block name profile_file_1
  rule name rule1
   file-type pre-defined name DOC PPT XLS MSOFFICE DOCX PPTX XLSX PDF VSD MPP
   file-type pre-defined name ODS ODT ODP EML UOF RAR TAR ZIP GZIP CAB
   file-type pre-defined name BZ2 Z 7ZIP JAR C CPP JAVA VBS
   application all
   action block
  rule name rule2
   file-type pre-defined name EXE MSI RPM OCX A ELF DLL PE SYS
   application all
   direction download
   action block
 profile type file-block name profile_file_2
  rule name rule1
   file-type pre-defined name EXE MSI RPM OCX A ELF DLL PE SYS
   application all
   action block
 #
 keyword-group name key1
  pre-defined-keyword name bank-card-number weight 1
  pre-defined-keyword name credit-card-number weight 1
  pre-defined-keyword name social-security-number weight 1
  pre-defined-keyword name id-card-number weight 1
  pre-defined-keyword name confidentiality weight 1
  user-defined-keyword name 公司违规信息
   expression match-mode text 违规信息
 #
 profile type data-filter name profile_data_1
  rule name rule
   keyword-group name key1
   file-type all
   application all
   action block
```





profile type mail-filter name profile_mail_1 rbl-filter enable send-mail anonymity action block send-mail attachment max-size 2048 action block recv-mail anonymity action block recv-mail attachment max-size 2048 action block # security-policy ning. huamei.com/cr rule name to_Internet policy logging session logging source-zone trust destination-zone isp1 source-address 10.1.11.0 mask 255.255.255.0 profile app-control profile_app_1 profile data-filter profile_data_1 profile file-block profile_file_1 profile mail-filter profile_mail_1 action permit rule name to_intra_server source-zone isp1 destination-zone trust destination-address 10.1.32.0 mask 255.255.255.0 profile file-block profile_file_2 profile mail-filter profile_mail_1 action permit

return



2 NIP 入侵阻断实验

- 2.1 实验介绍
- 2.1.1 关于本实验

入侵防御是一种安全机制。设备通过分析网络流量来检测入侵,并通过一定的 响应方式实时地中止入侵行为。本实验介绍如何配置入侵防御功能,保护企业 内部用户免受来自 Internet 的攻击。

2.1.2 实验目的

内网用户可以访问 Internet。该企业需要在 NIP 上配置入侵防御功能, 具体要求如下:

- 企业经常受到蠕虫、木马和僵尸网络的攻击,必须对这些攻击进行防范。
- 避免内网用户访问 Internet 的 Web 服务器时受到攻击。例如,含有 恶意代码的网站对内网用户发起攻击。

2.1.3 实验拓扑图



图2-1 安全设备管理实验拓扑图



2.1.4 前提条件

- 1. 配置防火墙网络连接、IP 地址、接口安全区域。
- 2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
- 3. NAT 策略部署完成。

2.1.5 实验任务列表

序号	任务	任务说明
1	配置入侵防御配置文 件	创建入侵防御配置文件,配置签名过滤 器。
2	提交入侵防御配置	提交配置。
3	配置安全策略	配置从Trust到Untrust的域间策略。
4	保存配置	查看并导出威胁日志。

2.2 实验任务配置

2.2.1 配置思路

- 1. 配置安全区域,完成网络基本参数配置。
- 2. 配置入侵防御配置文件 profile_ips_pc,保护内网用户。通过配置 签名过滤器来满足安全需要。
- 3. 创建安全策略 policy_sec_1, 并引用安全配置文件 profile_ips_pc, 保护内网用户免受来自 Internet 的攻击。

2.2.2 配置步骤

步骤1 配置入侵防御配置文件。

创建入侵防御配置文件 profile_ips, 配置签名过滤器。



a. 选择"对象 > 安全配置文件 > 入侵防御"。

Huawei	日本 二二 通板 監控		■ 7 对象	. 十 . 网络	里 系统			È	当前用户: admi	n 提交 保存	帮助 关于 创	跋密码 注销
 □ 副 证书 ● 地址 ● 地址 ● 地址 ● 地址 ● 地区 ② 服务 ◇ 広用 ○ 該通路券 ○ 該通路券 ○ 該金融置文件 ● 気感病却 ● 入島病毒 ● 入島があ ● 入島があ 	A 儲防的和正面文件 ◆ 新建 第 粉涂 腳頁 配置文件支更之后(※ 第 Strict web_server dis_server dis_server mail_server mail_server outside_frewall dds default	割 (Q)重高达名过滤料 要提交后才能生效。 類述 1页 > 2 範页型	4.第 次击取证 示宗赦 50	を称 default	对象 全部 全部 全部 全部 全部 全部 全部 全部 全部 全部 全部 全部 全部	严重性高高高高高高高高高高高高高高	送名 但作系统 Unix-like, Unix-like,	达维器 度用程序 全部 全部 全部 全部 全部 全部 全部 全部 全部 全部 全部 全部 全部	协议 全部 DNS, HTTP, DNS, SMB, DNS DNS, IMAP. DNS, HTTP, DNS, HTTP, 全部 全部	威胁失初 全部 	功作 昭断 采用登 采用登 采用登 采用登 采用登 告書 采用登 告書 采用登 告書 采用登 日	 ● 時新 思想场名检 *
								-11-	/	C	U控制台	

b. 配置入侵防御参数。





新建签名过滤器			? ×
	■ ■ 网络服务类协议 □ DNS □ TTP	~	^
威胁类别	 ◆ 全部 ◆ 病毒 ◆ 木马 ◆ 僵尸网络 ◆ 间谍软件 ◆ 广告软件 ◆ CG政击 ◆ 跨站脚本攻击 		
动作设置	 采用签名的缺省动作 告警 阻断 		
防火墙联动	关闭	SWC	~
		预览签名过滤结果 确定	取消

c. 单击"确定",完成入侵防御配置文件的配置。

步骤2 提交入侵防御配置。

单击界面右上角的"提交",在弹出的对话框中单击"确定"。

步骤3 配置安全策略。

a. 选择"策略 > 安全策略",单击"新建",按如下参数配置从 Trust 到 Untrust 的域间策略。

新建安全策略				1	? ×
提示:新建时可以基于策略模板来快速定 名称	义您需要的策略。[选择策略模板] policy_sec		*		^
描述	NONE				
VLAN ID	NONE	~	<1-4094>		
源安全区域	trust	~	[多选]		
目的安全区域	untrust	~	[多选]		
源地址/地区 🕐	请选择或输入地址]		
目的地址/地区 🕐	请选择或输入地址				
服务	请选择服务]		
应用	请选择应用或应用组		[多选]		
时间段	请选择时间段	\sim			
动作	● 允许	○ 禁止	al		
内容安全 反病毒	NONE	~	[][[]][[]][[]][[]][[]][[]][[]][[]][[]]		
入侵防御	profile_ips	~	[[[[]]]][[]]][[]]][[]]][[]]][[]]][[]][[]]][[]][[]]][[]][[]][[]]][[][]		
APT防御	NONE	\checkmark	酉(置)		
URL过滤			[四][[]]		~
			[确定取》	肖

b. 单击"确定"。



步骤4 保存配置。

单击界面右上角的"保存",在弹出的对话框中单击"确定"。

步骤5 结果验证。

在"监控 > 日志 > 业务日志"中,管理员可以定期查看类型为"入侵"的威胁日 志信息。

2.3 配置参考

#

sysname NIP

#

firewall defend action discard

#

undo dataflow enable

#

sa force-detection enable

#

engine-mode warning

#

earning. huamei.com/cr firewall dataplane to manageplane application-apperceive default-action drop #

time-range worktime

period-range 08:00:00 to 18:00:00 working-day

#

interface GigabitEthernet1/0/2

portswitch

undo shutdown

port link-type trunk

port trunk allow-pass vlan 2 to 4094

detect-mode inline

#

interface GigabitEthernet1/0/3

portswitch

undo shutdown

port link-type trunk

port trunk allow-pass vlan 2 to 4094

detect-mode inline

#

firewall zone local



set priority 100 # firewall zone trust set priority 85 add interface GigabitEthernet0/0/0 add interface GigabitEthernet1/0/0 add interface GigabitEthernet1/0/2 add interface GigabitEthernet1/0/4 # firewall zone untrust set priority 5 add interface GigabitEthernet1/0/1 add interface GigabitEthernet1/0/3 add interface GigabitEthernet1/0/5 # firewall zone dmz set priority 50 # profile type ips name profile_ips signature-set name profile_ips os unix-like windows android ios other target client severity high protocol HTTP category all application all # profile type url-filter name default # sa # pair-interface name g1/0/2_to_g1/0/3 pair GigabitEthernet1/0/2 GigabitEthernet1/0/3 # security-policy rule name ips_default disable profile ips default action permit rule name policy_sec source-zone trust destination-zone untrust



profile ips profile_ips action permit # return



了 应用服务器防病毒攻击实验

- 3.1 实验介绍
- 3.1.1 关于本实验

企业内部用户位于 Trust 区域,应用服务器(SMTP 邮件服务器)位于 Trust 区域, Internet 上的用户位于 ISP 1 区域,企业内网用户和 Internet 上的用户使用 SMTP 服务器发邮件。

在 FW 上配置 AV 功能,扫描企业内网用户和 Internet 上的用户的 SMTP 邮件中的附件,如果发现用户邮件的附件中带有病毒,则删除附件内容并在邮件正 文添加宣告,避免 SMTP 邮件服务器受病毒攻击。

- 3.1.2 实验目的
 - 掌握网关邮件反病毒的工作原理及配置方法;
 - 了解 SMTP 的工作原理;

3.1.3 实验拓扑图







3.1.4 前提条件

- 1 配置防火墙网络连接、IP 地址、接口安全区域。
- 2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
- 3 NAT 策略部署完成。

3.1.5 实验规划

PC 机两台、Mail 服务器	器一台,交换机一台,USG 系列防火墙 1 台。	
按照如卜规划配置买验	°	
	表3-1 策略名称规划	
名称	备注	
安全策略: av_mail	 允许 ISP 1 区域和 Trust 区域的 SMTP 服务和 POP 3 服务互访; 	
安全策略: mail	 放行 ISP 1 区域和 Trust 区域的 TCP 和 UDP 协 议; 	
安全配置文件:av_mail	 ISP 1 区域和 Trust 区域访问 SMTP 服务进行反 病毒; 	
邮件用户名: libai@security.com 密码: Huawei@123	• PC 1 上 foxmail 邮箱用户;	
邮件用户名: dufu@security.com 密码: Huawei@123	● PC 9 上 foxmail 邮箱用户;	

3.1.6 实验任务列表

序 号	任务	子任务	备注
	安全区域配置	将各接口划分入安全区域;	
1	配置基础数 据	中人体吸引型	允许ISP 1区域和Trust区域的SMTP 服务互访;
		女王來哈能直	放行ISP 1区域和Trust区域的TCP 和UDP协议;



		配置安全配置文件	ISP 1区域和Trust区域访问SMTP服 务进行反病毒配置;
2	配置反病毒	配置邮件删除附件 信息	在邮件正文中添加宣告信息;
		应用反病毒配置文 件	在安全策略smtp中应用反病毒配 置文件。

- 3.2 实验任务配置
- 3.2.1 配置思路



3.2.2 配置步骤

步骤1 配置 FW1 基本数据。(略)

步骤2 配置域间防火墙策略。



放行 ISP 1 区域和 Trust 区域的 TCP 和 UDP 协议,邮件的发送基于 TCP,收
 取基于 UDP。

廖叔女主宋昭				? ×
提示:新建时可以基于策略模板来快	速定义您需要的策略。[选择]	策略模板]	7	~
名称	mail	×	*	
描述				
策略组	NONE	~		
源安全区域	trust,isp1	~	[多选]	
目的安全区域	trust,isp1	~	[多选]	
源地址/地区 🕐	any]	
目的地址/地区🕐	any			
用户②	any		[多选]	
接入方式 🕐	any]	
终端设备 🕐	any			
服务	tcp udp			
应用	any		[多选]	
时间段	any	~		
动作	• 允许	○ 禁止		
内容安全				
反病毒	NONE		[置]]	
入侵防御	NONE		[配置]	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
LIBI 建油	NONE		[刑法]	

步骤3 配置反病毒。

配置反病毒配置文件。选择"对象 >安全配置文件 >反病毒"。在"反病毒配置文件"中单击"一新建",配置完成后单击"确定"。配置文件完成后单击"提交"。



修改反病毒配置	文件						?	×
名称	av_ma	ail			:	× *		~
描述						. 1		
攻击取证	自用 检测到病毒后,系统会在设备中获取包含该病毒的数据包。您可以在日志中查看数据包内容。							
联动检测	启用	开启该功能 配置文件,	《后,会导致病毒 联动检测功能才	™检测的性能降低。 ↑会生效。	安全策略中需要	同时引用反病毒和	D <mark>AP</mark> T防御	
H- 25	文件传	输协议		邮件协议		共享	协议	
94 4U	HTTP	FTP	SMTP	POP3	IMAP (?)	NFS(?)	SMB (?)	
上传			✓					
下载								
动作	阻断 🗸	阻断 🗸	宣告 🗸	告警 🗸	告警	告藝	阻断	
应用例外				病毒例外				
请选择应用名称		🔽 🔜 添加	🗱 删除	请输入病毒ID		📑 添加	1 💥 删除	
名称		动作		D		名称	0	
							0	
			没有记录			<u> </u>	没有记录	~
					0.		确定 取消	¥.

配置邮件删除附件信息。选择"系统 >配置 >推送信息配置"。在"邮件删除
 附件信息"中单击"下载模板",在下载后的模板中修改推送信息。然后单击
 "浏览"导入文件。

邮件删除附件信息		?	×
名称	邮件删除附件信息		
描述	删除病毒感染的邮件附件并添加删除信息。		
文件格式	ТХТ		
文件大小上限	1KB		
导入文件	浏览 下载模板		
✤推送信息中必须且只	有一个%FILE标识符。		
	导入即	消	

应用反病毒配置文件。选择"策略 >安全策略 >安全策略列表"。配置安全策略,并单击安全策略"mail"的"内容安全"模块选择反病毒配置文件"av_mail"。



HCNP-Security CSSN 实验指导手册

修改安全策略			? ×
提示: 新建时可以基于策略模板	反来快速定义您需要的策略。[<mark>选择策略</mark> 移	真板]	~
名称	mail	*	
描述			
策略组	NONE	~	
源安全区域	trust,isp1	[多选]	
目的安全区域	trust,isp1	[多选]	
源地址/地区🕐	any		
目的地址/地区(?)	any		
用户②	any	[多选]	
接入方式(?)	any		
终端设备 🕐	any		
服务	smtp pop3		1 (
应用	any	[多选]	
时间段	any	~	
动作	● 允许	○ 禁止	
内容安全		*	
反病毒	av_mail	[置酒]	
入侵防御	NONE	[置酒]	~
HRI 计准	NONE	[两] [两] [两] [两] [两] [元] [元] [元] [元] [元] [元] [元] [元] [元] [元	

3.3 结果验证

在 PC 1 和 PC 9 上相互用 foxmail 发送附件含有病毒的邮件和正常的邮件,查看结果。

正常收发邮件

	🛹 发送 🕒 保存 🥔 附件 🖃 超大附件 💌 图片 🛄 截屏	libai@security.com → 🛛 🗄
-12-14 -12-14	wtth: dufu <dufu@security.com>; by: ±50: normal verdana 10 A + □ + B I I:bai@security.com</dufu@security.com>	
	normal.txt IKB	



💪 normal	> 转发 🔹 💙 删除	🔊 邮件标签	🚍 打印	🔲 打印预览	_ □ X » ↑ ↓ ☷
normal ★					
libai@security.com 发给 dufu					2017-07-13 10:39 ????
normal.txt (12 B)					
FYI.					
libai@security.com					
					1 Cr
					colu,
发送病毒附件					









3.4 配置参考

3.4.1 FW 的配置

[FW1]display current-configuration

sysname FW1

#

#

firewall detect ftp

#

firewall zone local

set priority 100

#

firewall zone trust

set priority 85

add interface GigabitEthernet1/0/1



#

firewall zone name isp1 id 4

set priority 40

add interface GigabitEthernet1/0/4

#

learning huanet.com/cr profile type av name av_mail

undo http-detect

undo ftp-detect

smtp-detect action declare

undo pop3-detect

undo imap-detect

undo nfs-detect

undo smb-detect

#

sa

#

security-policy rule name mail source-zone trust source-zone isp1 destination-zone trust destination-zone isp1 service smtp service pop3 profile av av_mail action permit #

return



4 内容用户防病毒攻击实验

4.1 实验介绍

4.1.1 关于本实验

企业内部用户位于 Trust 区域,应用服务器(HTTP 服务器)位于 DMZ 区域, 在 FW 上配置 AV 功能,当内网用户访问的网页带病毒时,USG2200 中断访 问,并向用户推送一个警告页面提示访问的网页中含病毒。

4.1.2 实验目的

- 掌握内部用户访问 Internet 上的网页时反病毒的工作原理及配置方法;
- 4.1.3 实验拓扑图



图4-1 内网用户防病毒攻击实验拓扑图



- 4.1.5 前提条件
 - 1. 配置防火墙网络连接、IP 地址、接口安全区域。
 - 2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
 - 3. NAT 策略部署完成。
- 4.1.6 实验规划

PC 机一台、WWW 服务器一台,交换机一台,USG 系列防火墙 1 台。 按照如下规划配置实验。

表4-1 策	略名称规划
--------	-------

	名称	备注		
	安全策略: http	 允许 Trust 区域访问 ISP 1 区域的 Http 服务; 		
	地址池: http	• PC 1 用于源 NAT 的地址池;		
	安全配置文件: av_http	 Trust 区域访问 ISP 1 区域的 http 阻断病毒; 		

4.1.7 实验任务列表

序 号	任务	子任务	备注
1	配置反病毒	配置安全配置 文件	对Trust区域访问ISP 1区域的Http服务 进行反病毒配置;



		配置病毒文件 阻断信息	配置web阻断推送信息;
		提交反病毒配 置	反病毒配置需提交;
2	配置安全策 略	安全策略配置	允许Trust区域访问ISP 1区域的Http服 务;在安全策略http中应用反病毒配 置文件;

- 4.2 实验任务配置
- 4.2.1 配置思路



4.2.2 配置步骤

步骤1 配置反病毒。

配置反病毒配置文件。选择"对象 >安全配置文件 >反病毒"。在"反病毒配置文件"中单击"✤ 新建",配置完成后单击"确定"。配置文件完成后单击"提交"。



修改反病毒配置	文件							?	×
名称	av_htt	av http							
描述									
攻击取证	自用	检测到病毒 容。	¥后,系统会在设	备中获取包含该病	毒的数据包。您可		看数 据包内		
联动检测	启用	开 启该功能 配 置文件,	《后,会导致病毒 联动检测功能才	检测的性能降低。 会生效。	安全策略中需要同	同时引用反病毒和	和APT防御		
14. Sh	文件传	输协议		邮件协议		共同	家协议		
190-192	HTTP	FTP	SMTP	POP3	IMAP (?)	NFS(?)	SMB (?)		
上传									
下载									
动作	阻断 🗸	阻断 🗸	告整 🗸	告警 🗸	告警	告警	阻断		
应用例外				病毒例外					
请选择应用名称		🔽 🔜 添加	💢 刪除	请输入病毒ID		🔜 添力	0 🐹 刪除		
名称		动作		ID		名称			
			没有记录	, dh			没有记录		~
							确定取	消	

配置病毒文件阻断信息。选择"系统 >配置 >推送信息配置"。在"病毒文件
 阻断配置"中单击"下载模板",在下载后的模板中修改推送信息。然后单击
 "浏览"导入文件。

病毒文件阻断配置		?	×
名称 描述 文件格式 文件大小上限 导入文件	病毒文件阻断配置 表示访问的WEB页面有病毒,页面被阻断时推送的页面。 TXT、HTML 21KB 浏览 下载模板		
✤请您确保导入文件	内容的安全性,防止推送页面中包含钓鱼网站或木马等恶意信息。		
	导入	又消	

提交反病毒配置。



提交	×	
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@		
	确定取消	

步骤2 配置域间防火墙策略。

配置安全策略 http, Trust 域用户可以访问 ISP 区域的 WWW 服务器;应 用反病毒配置文件,选择"策略 >安全策略 >安全策略列表"。单击安全 策略"http"的"内容安全"模块选择反病毒配置文件"av_http"。

	修改安全策略			? ×	
	提示: 新建时可以基于策略模板来快速定义	《您需要的策略。[选择策略模板]	7.	~	
	描述	av_http ×			
	策略组	NONE			
	源安全区域	trust	• [多选]		
	目的安全区域	isp1	• [多选]		
	源地址/地区?	any			
	目的地址/地区?	any			
	用户②	any	[多选]		
1/- -	接入方式③	any			
F.K	终端设备 🕑	any			l
13-	服务	any			
, 10	应用	any	[多选]		
	时间段	any			
7	动作	 允许 一 禁止 			
	内容安全	av http	[m)罢1		
	入侵防御				
				~	,
			确定 耳	[] 消	



4.3 结果验证

在 PC1 上打开 IE 浏览器, 输入"http://10.1.92.80", 查看页面显示。

在 FW1 上选择"监控 > 日志 > 业务日志",查看防火墙日志。

安全组	吸别	日志类型	时间	日志源	描述
0 8	浩	VIRUS	2017/11/1 19:55:13	FW1 %%01AV/4/VIRUS(1)[0]:	AV检测发现病毒。(日志序号=8,虚拟系统="public",安全策略="av_http"…

4.4 配置参考

4.4.1 FW 1 的配置

learning. huamei.com/cr <FW1>display current-configuration

#

sysname FW1

#

firewall detect ftp

#

firewall zone local

set priority 100

#

#

firewall zone trust

set priority 85

add interface GigabitEthernet1/0/1

firewall zone name isp1 id 4

set priority 40

add interface GigabitEthernet1/0/4

#

profile type av name av_http

http-detect direction download

undo ftp-detect

undo smtp-detect

undo pop3-detect



undo imap-detect undo nfs-detect undo smb-detect # sa Ethorning huanei. com cr #



)防火墙单包攻击防范实验

- 5.1 实验介绍
- 5.1.1 关于本实验

在 DoS 攻击中,单包攻击也是不可小觑的一类威胁,通过在防火墙上启用单包 攻击防范功能,可以有效的防止由恶意用户发起的单包攻击。本实验将在防火 墙上配置单包攻击防范策略,验证其对此类攻击的防范效果。

5.1.2 实验目的

配置防火墙网络层单包攻击策略,防止外部恶意用户攻击内网资源。

5.1.3 实验拓扑图



图1-11 防火墙单包攻击防范实验拓扑图

5.1.4 前提条件

4. 配置防火墙网络连接、IP 地址、接口安全区域。

004	- 4	4 00
201	7-1	1-23

华为保密信息,未经授权禁止扩散



- 5. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
- 6. NAT 策略部署完成。

5.1.5 实验任务列表

序号	任务	子任务
	配置防火墙单包攻击防范策 略	启用防火墙单包攻击中的防范策 略。
1	查看日志	在防火墙上查看攻击防范日志, 确认防火墙是否阻挡了攻击行 为。
任务配置		. 12Wei
置步骤		
1 基本配置	٥	

- 5.2 实验任务配置
- 5.2.1 配置步骤
 - 步骤1 基本配置。

配置网络连接、IP 地址、接口安全区域及包过滤, 放行 isp1/isp2 访问 Trust 区 域的流量(具体过程省略)。

步骤2 配置防火墙单包攻击策略。

选择"策略 > 安全防护 > 攻击防范",单击"单包攻击"页签,设置"防范动作" 为告警。并配置其余防护策略如下图所示:



Anti-DDoS 单包攻击		
防范动作 💿 告警	○ 丢弃	
配置扫描类攻击防范		
✔ 地址扫描		
最大扫描速率	4000	<1-10000>包秒
黑名单老化时间	20	<1-1000>分钟
✔ 端口扫描		
最大扫描速率	4000	<1-10000>包/吵
黑名单老化时间	20	<1-1000>分钟
配置畸形报文类攻击防范		
✓ IP欺骗攻击防范	🗌 IP分片报文检测	Teardrop
🖌 Smurf	🖌 Ping of Death	Fraggle
WinNuke	Land	TCP报文标志合法性检测
配置特殊报文控制类攻击防范		
✓ 超大ICMP报文控制		
最大长度	4000	<28-65535>字节
□ ICMP不可达报文控制	✔ ICMP重定向报文控制	Tracert
□ 源站选路选项IP报文控制	□ 路由记录选项IP报文打	空制 时间戳选项IP报文控制
	应用	

5.3 结果验证

5.3.1 查看防火墙的日志

当防火墙检测到攻击行为后,可通过查看日志了解攻击细节。

(特别提醒:此处已使用模拟软件进行攻击测试。模拟软件仅用于攻防演练及教 学测试用途,禁止非法使用。)

选择"监控 > 日志 > 业务日志",可查看到防火墙拦截的攻击行为。

业务日志列表				
🛃 导出				🖏 刷新 请选择安全级别 💟 🔍 查询
安全级别	日志类型	时间	日志源	描述
• 警告	FIREWALLATCK	2017/9/20 14:13:28	FW1 %%01ATK/4/FIR	攻击类型="Tear drop attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/4 ", 协议="ICMP", 攻击源
• 警告	FIREWALLATCK	2017/9/20 14:12:58	FW1 %%01ATK/4/FIR	攻击类型="Tear drop attack", <mark>槽</mark> 位号=" ", CPU号="0", 接收接口="GE1/0/4 ", 协议="ICMP", 攻击源
警告	FIREWALLATCK	2017/9/20 14:12:28	FW1 %%01ATK/4/FIR	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议="UDP", 攻击源地
警告	FIREWALLATCK	2017/9/20 14:10:28	FW1 %%01ATK/4/FIR	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议="UDP", 攻击源地
警告	FIREWALLATCK	2017/9/20 14:09:58	FW1 %%01ATK/4/FIR	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议="UDP", 攻击源地
() 警告	FIREWALLATCK	2017/9/20 14:07:58	FW1 %%01ATK/4/FIR	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议="UDP", 攻击源地
() 警告	FIREWALLATCK	2017/9/20 14:07:28	FW1 %%01ATK/4/FIR	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议="UDP", 攻击源地
() 警告	FIREWALLATCK	2017/9/20 14:02:58	FW1 %%01ATK/4/FIR	
() 警告	FIREWALLATCK	2017/9/20 14:02:28	FW1 %%01ATK/4/FIR	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议="UDP", 攻击源地
() 警告	FIREWALLATCK	2017/9/20 14:01:58	FW1 %%01ATK/4/FIR	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议="UDP", 攻击源地
警告	FIREWALLATCK	2017/9/20 13:59:27	FW1 %%01ATK/4/FIR	攻击类型="IP spoof attack", 槽位号=" ", CPU号="0", 接收接口="GE1/0/1 ", 协议="TCP", 攻击源地



5.4 配置参考

5.4.1 FW1 的配置

#

firewall defend port-scan enable firewall defend ip-sweep enable Et the the interning huave contor firewall defend teardrop enable





防火墙流量型攻击防范实验

- 6.1 实验介绍
- 6.1.1 关于本实验

流量型攻击是 DDoS 攻击中最主要的攻击类型。通过在防火墙上启用 Anti-DDoS 功能,可以有效的防止由恶意用户发起的流量型攻击。本实验将在防火墙上配置 DDoS 攻击防范策略,验证其对此类攻击的防范效果。

6.1.2 实验目的

配置防火墙 SYN Flood 攻击防范策略,防止外部恶意用户攻击内网资源。

6.1.3 实验拓扑图



图 2-1 防火墙流量型攻击防范实验拓扑图

6.1.4 前提条件

1. 配置防火墙网络连接、IP 地址、接口安全区域。



- 2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
- 3. NAT 策略部署完成。

6.1.5 实验任务列表

序号	任务	子任务	
	配置防火墙Anti-DDoS防范策 略	配置SYN Flood防范策略。	
1	查看日志	在防火墙上查看攻击防范日志, 确认防火墙是否阻挡了攻击行 为。	
任务配置		, 18Mei .	
置步骤			
1 基本配置			

- 6.2 实验任务配置
- 6.2.1 配置步骤

步骤1 基本配置

配置网络连接、IP 地址、接口安全区域及包过滤(具体过程省略)。

- 步骤 2 配置防火墙 Anti-DDoS 防御模式及接口。
 - 1. 选择"策略 > 安全防护 > 攻击防范",在 Anti-DDoS 页签下,配置"防御模 式"为检测,选择 G1/0/4 及 G1/0/5 接口为检测接口。

Anti-DDoS 单包攻击			
防御模式	 ● 检测 ● 描述 		
接口	可迭 GE0/0/0(GE0/MGMT) GE1/0/0 GE1/0/1 GE1/0/2 GE1/0/3	>> <<	已迭 GE1/0/4 GE1/0/5
	K < 第 1 页共1页 > ∑		
ATIC联动	□ 启用		

2. 在 DDoS 栏, 点击"配置学习参数", 启用流量学习功能。学习周期为每 天,每次学习1小时。配置完成后,点击"确定"。



配置学习参数				? ×
启用"学习功能"后,系统将自动 结果将显示在"DDoS"界面的" 面中勾迭"自动应用"的"启用",	动分析当前流量并 学习结果"列中。; 将学习结果自动	并计算出各种项 您可以参考该 的应用到阈值中	\去类型的建议防须 结果手工设定阈值 □。	范阈值。计算 ,或者在本界
学习功能	✔ 启用			
每次学习时长	1 <1-	24>	小时 🗸	
学习模式	○ 单次学习	۲	周期学习	
周期学习间隔	1 <1-	365≻	天 🗸	
自动应用	启用			
学习容忍度	50 <0-	4000>		
			确定	取消

3. 选择启用 SYN Flood 攻击防范技术。保持默认阈值。配置完成后点击"应 用"。

DDoS	No.			
📓 配置学习参数 📓 应用学习结果				
学习状态:正在学习				
攻击类型	防范技术	启用		讕值
SYN Flood	源探测	2	2000	<1-80000000>pps
	指纹防范		50	<1-10240>Mbps
UDP Flood	分片指纹防范		50	<1-10240>Mbps
	限流		50	<1-10240>Mbps
ICMP Flood	限流		2000	<1-1200000>pps
HTTP Flood	●基础源探测 C 302重定向 C 高级源探测		8000	<1-80000000>pps
HTTPS Flood	源探测		2000	<1-8000000>pps
DNS Request Flood	●源探则 CCNAME重定向③		2000	<1-80000000>pps
DNS Response Flood	源探测		2000	<1-80000000>pps
SIP Flood	源探测		2000	<1-80000000>pps
	应用			

6.3 结果验证

6.3.1 查看防火墙的日志

当防火墙检测到攻击行为后,可通过查看日志了解攻击细节。

特别提醒:此处已使用模拟软件进行攻击测试。模拟软件仅用于攻防演练及教 学测试用途,禁止非法使用。

选择"监控 > 日志 > 业务日志",可查看到防火墙拦截的攻击行为。



业务日志列表						
局				🖓 刷家	请选择安全级别	~ (
安全级别	日志类型	时间	日志源	描述		
• 警告	FIREWALLATCK	2017/9/20 15:14:58	FW1 %%01ATK/4/FIREWALLATCK(I)[0]:	攻击类型="IP spoof attack", 槽位号=" "	, CPU号="0", 接收接口="G	E1/0/1 ",
• 警告	FIREWALLATCK	2017/9/20 15:14:58	FW1 %%01ATK/4/FIREWALLATCK(I)[1]:	攻击类型="Syn flood attack", 槽位号="	", CPU号="0", 接收接口="0	€1/0/4 ", †
警告	FIREWALLATCK	2017/9/20 15:14:28	FW1 %%01ATK/4/FIREWALLATCK(I)[2]:	攻击类型="IP spoof 攻击类型="Syn fl 문-"0" 按此按口:	ood attack", 槽位号=" ", CP ="GE1/0/4 " 执论="TCP" 1	いたり
警告	FIREWALLATCK	2017/9/20 15:13:58	FW1 %%01ATK/4/FIREWALLATCK(I)[3]:	攻击类型="IP spoof 址="10.1.93.193	10096 10.1.93.195:10098	10.1.93.1
警告	FIREWALLATCK	2017/9/20 15:12:58	FW1 %%01ATK/4/FIREWALLATCK(I)[4]:	攻击类型="IP spoof 1.93.199:10001	10.1.93.200:10002 10.1.93	3.201:100
警告	FIREWALLATCK	2017/9/20 15:07:58	FW1 %%01ATK/4/FIREWALLATCK(I)[5]:	攻击类型="IP spoof 2:10004 ",攻击目	1000510.1.93.204:10006 1的地址="10.1.71.11 ", 攻击	10.1.93.20 5开始时
警告	FIREWALLATCK	2017/9/20 15:04:58	FW1 %%01ATK/4/FIREWALLATCK(I)[6]:	p击类型="IP spoof 间="2017-9-201 间="2017-9-201	5:14:35", 攻击结束时 5:14:57", 攻击报文个	
• 警告	FIREWALLATCK	2017/9/20 15:04:28	FW1 %%01ATK/4/FIREWALLATCK(I)[7]:	攻击类型="IP spoof 数="1528993", 政击类型="IP spoof 作="discard".	マ击速率="73614",用户="",;	动
警告	FIREWALLATCK	2017/9/20 15:03:58	FW1 %%01ATK/4/FIREWALLATCK(I)[8]:	攻击类型="IP spoof attack", 槽位号=" "	, CPU号="0", 接收接口="G	E1/0/1 ",
• 警告	FIREWALLATCK	2017/9/20 15:02:58	FW1 %%01ATK/4/FIREWALLATCK(I)[9]:	攻击类型="IP spoof attack", 槽位号=" "	, CPU号="0", 接收接口="G	Ē1/0/1 ",
1 的配置	묘					
, HJDCE	1					
ŧ						
nterface	GigabitEthe	rnet1/0/4				
nti-ddoc	flow-statist	ic anabla				
inti-uu0s	ทบพารเลเรเ					
ŧ						
nterface	GigabitEthe	rnet1/0/5				
nti-ddoc	flow-statist	ic anabla				
init-uu0s	now-statist					
ŧ						
anti-ddo	s syn-flood	sourco-dotoc	+			

6.4 配置参考

6.4.1 FW1 的配置

anti-ddos syn-flood source-detect anti-ddos baseline-learn start anti-ddos baseline-learn mode loop anti-ddos baseline-learn learn-duration 60 anti-ddos baseline-learn learn-interval 1440